METHOD AND ARRANGEMENT IN A COMMUNICATION NETWORK

FIELD OF INVENTION

The present invention relates to the field of communication networks and more specifically to an ad hoc communication network and a method for establishing security in an ad hoc network.

DESCRIPTION OF RELATED ART

The fast growth of open networks with easy access has raised many security problems. Several security solutions for public networks like the Internet have appeared. Security is a problem in all kinds of open networks both wired and wireless. Information transmitted over the air is extremely vulnerable. Today there exist solutions that are built upon some type of so called *public key infrastructure* (PKI). A public key infrastructure is a system used to distribute and check public keys that can be used to authenticate users, exchange session keys, sign information or encrypt information.

In a PKI system, two corresponding (also called asymmetric) keys are used in connection with protecting information. Information, which is encrypted with one of the two keys, can be decrypted only with the other key. In some PKI systems either of the two keys can be used to encrypt and the other to decrypt. In other systems, one key must be used only for encryption and the other for decryption. One important feature of PKI systems is that it is computationally unfeasible to use knowledge of one of the keys to deduce the other key. In a typical PKI system, each of the systems possesses a set of two such keys. One of the keys is maintained private while the other is freely published. If a sender encrypts a message with the recipient's public key, only the intended recipient can decrypt the message, since only the recipient is in possession of the private key corresponding to the published public key. If the sender, before performing the above

encryption, first encrypts the message with the senders private key, the recipient, upon performing first a decryption, using the recipient's private key, then a decryption on the result, using the sender's public key, is assured not only of privacy but of authentication since only the sender could have encrypted a message such that the sender's public key successfully decrypts it. In one digital signature scheme, one-way hash is first applied to a message and the hash of the message is encrypted with the sender's private key.

A PKI distributes one or several public keys and determine whether a certain public key can be trusted for certain usage or not. A piece of digitally signed information is often called a certificate. Certificates are the basis upon which PKIs are built.

The degree of confidence that the recipient has in the source of a message depends on the degree of the recipient's confidence that the sender's public key corresponds to a private key that was possessed only by the sender. In many current systems, a number of generally well trusted certification authorities have been established to provide this degree of confidence.

A common certificate format is Standard X.509 (developed by the International Standards Organisation (ISO) and the Comité Consultatif Internationale Telegraphique et Telephonique (CCITT)). Such a certificate may, e.g., include a public key, the name of subject who possesses or is associated with the public key, an expiration date, all of which are digitally signed by a trusted party. The digital signature may be provided e.g., according to the digital signature standard (DSS) (National Institute of Standards and Technology (NIST)). Typically a digital signature involves applying a one-way hash and then encrypting with the private key of, in this case, the certification authority. Such digital signature is provided using the private key of the trusted party which, in turn, is authenticated using the trusted party's certificate signed by yet another trusted party, so that there may be a multi-level hierarchy of trusted parties.

Another certificate format is Pretty Good Privacy (PGP) developed by P. Zimmermann and described in Internet Engineering Task Force (IETF) Open

PGP Specification. PGP provides a way to encrypt and decrypt, sign data and exchange keys. Thus it is more than just a PKI. However, the main idea with PGP is that no strict PKI is needed. Instead the PGP users themselves create and extend the PKI they need. This is done by certifying other users public keys, i.e., signing trusted public keys with their own secret key. In this way a "web of trust" is created. A particular key may have several different user IDs. Typically a user ID is an email address. If a revocation signature follows a key, the key is revoked. A user certifies another users key by signing it with one of the keys of his own, which has signing capability. When signing another key, different trust levels can be set, i.e., the amount of confidence the signer has in the signed key and user ID.

Today, so-called ad hoc networks are used more and more frequently. An ad hoc network is established temporary for a special purpose. There is no fixed infrastructure, the nodes are the network. The nodes within the network are often mobile and using radio links. An ad hoc network might constitute dynamic wide area connectivity in situations such as military operations, rescue and recovery operations, and remote construction sites. An ad hoc network might also constitute local area connectivity in situations such as temporary conference sites, home networks and robot networks. An ad hoc network might also constitute personal area networks in situations such as interconnected accessories, ad hoc conference table and games. The nodes might consist of e.g. mobile phones, lap tops, television sets, washing machines In some situations like in military operations or business conferences when the communication between the nodes comprises secrets, it is very important that a sender of a message can trust that the receiver really is the intended receiver.

In the previous examples, bindings between public keys and names or authorisation are described. Several of these certificate solutions exist in different systems. However, it is not yet described how different certificates needed for different kinds of purposes are obtained. In the case of ordinary X.509 type of

PKI with hierarchical Certificate Authority (CA) structures, finding the right certificate is done using some central on-line server or by direct transmission of the certificate at connection set up. When using PGP either the desired public key is stored locally on a machine or the device has to make a connection to a central PGP server in order to find the desired pubic key. This works if it is possible for entities that need some type of security relation to have on-line connections to some particular servers. This is not the case for ad hoc networks. Ad hoc networks are created on the fly between entities that happen to be at the same physical location.

Therefore, what is further needed is a mechanism for checking if different nodes in an ad hoc network share a trust relation and for creating trust among a certain set of nodes without any pre-defined relations.

The problem of how to distribute trust using public keys in ad hoc networks is addressed in this invention. Still the existing PKIs provide a basis upon which solution also for ad hoc network can be built.

SUMMARY OF THE INVENTION

The present invention relates to the requirement of security in an ad hoc network. More particularly it relates to the problem within ad hoc networks, not having on-line connections to a particular server for getting desired public keys or certificates, required to create trust relations.

Accordingly, it is an object of the present invention to unravel the above-mentioned problem.

The aforesaid problem are solved by means of a method for finding possible trust relations between nodes within the ad hoc network and share them with other nodes within the ad hoc network.

The following scenario of establishing security in an ad hoc network describes the inventive concept of the present invention.

Within an ad hoc communication network, some of the nodes have a mutual trust relation to each other, thus constituting a trust group. A node within the network is being a candidate node for joining the trust group. An X-node is identified, being a member of a trust group and having a trust relation with the candidate node. The X-node distributes trust relations between the members of the trust group and the candidate node.

An advantage of the present invention is it is possible to achieve the necessary security associations needed for distributing and sharing information among a group of users that happens to be at the same physical location. There are a large amount of applications that fits in to this scenario. Among those can be mentioned people from different companies or organisations that gather in a conference room can share documents with the meeting members.

Another advantage of the present invention is that the number of manually created trust relations between members in an ad hoc communication network is decreased.

Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a scenario where a single node establishes trust with an existing trust group within a communication network.

Figure 2 shows a scenario where trust is established in an ad hoc communication network.

Figure 3 shows a scenario where trust is established in an ad hoc communication network.

Figure 4 shows a scenario where two trust groups within an ad hoc communication network are merged.

Figure 5 shows a scenario where two trust groups within an ad hoc communication network are merged.

Figure 6 shows a scenario where two trust groups within an ad hoc communication network are merged.

Figure 7 shows a scenario where two trust groups within an ad hoc communication network are merged.

DESCRIPTION OF PREFFERED EMBODIMENTS

The ad hoc communication network according to the invention constitutes e.g. a bluetooth network. The ad hoc network comprises nodes constituting e.g., laptops and mobile phones, each node comprising a receiver and a computer, the computer comprising a processor and a memory. The nodes are interconnected via communication links.

Figure 1 shows a possible scenario of the present invention in which a single node 101 is added to an existing trust group 102. The trust group 102 comprises nodes 103-105. All the nodes 103-105 in the trust group 102 have mutual trust relations with each other, the trust relations being created with trusted public keys. Thus each node 103-105 in the trust group 102 has the trusted public keys of all

the other nodes 103-105 within the trust group 102. The trusted public keys are e.g. used to sign messages to be sent between trusted nodes. The single node 101 and the trust group constitute an ad hoc communication network 106. According to the invention all nodes 101, 103-105 have authority to delegate trust to other nodes that they trust within the network. The single node 101 would like to join the trust group 102 and the single node is from now on called the candidate node 101.

Either the candidate node 101 sends a broadcast message to all the nodes 103-105 within the trust group or it unicasts message to a special look up server where all the nodes 103-105 can obtain the message. The message comprises the public key that the candidate node 101 wants to use. The message might comprise a set of public keys that the candidate node 101 wants to use and possible certificate/s certifying the public key/s.

Each node 103-105 within the trust group 102 obtains the public key of the candidate node 101, and checks if it trusts the public key of the candidate node.

A node 103 within the trust group that trusts the public key of the candidate node 101 is identified, a so-called X-node 103. The X-node,

- sends a signed message comprising all the trusted keys of the nodes 103-105 within the trust group 102 to the candidate node 101, and
- signs the public key of the candidate node 101 and sends a message comprising the key together with the signature to all the other nodes 104, 105 within the trust group 102.

If none of the nodes 103-105 within the trust group 102 trusts the candidate node a trust relation has to be manually created with an arbitrary node 105 within the trust group 102. This node 105 thus constitutes an X-node. A manual creation of trust relation between two nodes can be performed in different ways. In one way the two nodes enter their pin codes and then exchange public keys using an

authenticated channel. The manual creation of trust relations results in that each node obtains a trusted public key from the other party.

After the manual creation of trust, the X-node 105

- sends a signed message comprising all the trusted keys of the nodes 103-105 within the trust group 102 to the candidate node 101, and
- signs the public key of the candidate node 101 and sends a message comprising the key together with the signature to all the other nodes 103, 104 within the trust group 102.

Figure 2 shows another scenario of the present invention. In this scenario an ad hoc communication network 201 is formed. The trust groups 202, 203, 204 and 205 within the ad hoc network are used to create additional trust relations within the network. The trust relations are created with signed public keys. The ad hoc network comprises nodes A-M. In this embodiment, each of the nodes A-M constitutes a node being a candidate for joining a secure ad hoc network i.e., a trust group wherein all nodes A-M have mutual trust relations.

The nodes A, B, C, D and E have mutual trust relations and constitute a trust group 202.
The nodes D, E, G, J and K have mutual trust relations and constitute a trust group 203.
The nodes A, E, F and I have mutual trust relations and constitute a trust group 204.
The nodes H and M have mutual trust relations and constitute a trust group 205.
The node L has no trust relations to any of the other nodes within the network.

As shown in figure 2, the node E belongs to three trust groups 202, 203 and 204. The node D and E belong to two trust groups, 202 and 203. The nodes A and E belong to two trust groups 202 and 204.

According to the invention all nodes A-M have authority to delegate trust to other nodes that they trust, within the network. 201.

Each node A-M within the ad hoc network 201 sends a broadcast message to all the nodes A-M within the ad hoc network 201 or a unicast message to a special look up server where all the nodes A-M can obtain the message. The message comprises the public key that the candidate node A-M wants to use. The message might comprise a set of public keys that the candidate node wants to use and possible certificate/s certifying the public key/s.

Each of the nodes A-M obtains the public keys of all the other nodes A-M, either they are trusted or untrusted. Each node A-M then creates a list of its trusted nodes and their corresponding keys. E.g. node A which belongs to trust group 202 trusts the nodes B, C, D and E.

In this scenario, one node A is decided to act as a server node A. Each of the nodes B-M, sends a registration message to the server node A comprising its public key and the list of its trusted nodes and their corresponding public keys.

Using the obtained information the server node A identifies all the nodes A-M and the trust groups 202-205 within the ad hoc network.

Server node A might find that some nodes or some trust groups are isolated, i.e. neither having a trust relation with the server node A nor having a trust relation with any of the nodes that A has a trust relation with. In this embodiment that goes for node L and trust group 205 comprising the nodes H and M.

In that case server node A asks the node L, to manually create a trust relation with the server node A. Server node further A asks one node H in that trust group 205, to manually create a trust relation with the server node A. This results in two more

trust groups and is illustrated in figure 3. The nodes A and L constitutes trust group 301 and the nodes A and H constitutes trust group 302.

The server node A classifies all the nodes within the ad hoc network as being nodes that the server node A trusts, nodes B, C, D, E, F, I, H and L, i.e. sever-trusted nodes, or as being nodes that server node A not trust, nodes G, J, K and M, i.e. server-untrusted nodes. The server node A then makes a list comprising the server-untrusted nodes, the so-called untrust-list.

A server-trusted node trusting a server-untrusted node constitutes a so-called Y-node. The server node A identifies as many Y-nodes as required for distributing trust relations to all or as many as possible of the server-untrusted nodes. I.e. server node A identifies node D, having trust relations with nodes G, K and J, and node H having a trust relation with node M. Thus node D and node H can distribute trust relations between all the server-untrusted nodes and server node A according to the following process:

The server node A sends a message to the identified Y-nodes, the message comprising,

- the untrust-list comprising the nodes G, J, K and M and their corresponding public keys, and
- a request of distributing as many trust relations as possible between server node A and server-untrusted nodes.

An Y-node obtains the message and checks, which of the keys it trusts, i.e. which of the server-untrusted nodes G, J, K and M the Y-node trusts.

The identified Y-nodes then each perform the following steps 1-3 for each of the nodes that the respective Y-node trusts. In this case the Y-node D performs the steps for each of the nodes G, J and K and Y-node H performs the steps for node M.

1. The Y-node signs the public key of server node A and sends it to the node that the Y-node trusts, e.g. Node D signs server node A's key and sends it to node G,
2. The Y-node signs the public key of the node that the Y-node trusts and sends it to server node A, e.g. Node D signs node G's key and sends it to server node A.
3. Server node A reclassifies the node that the Y-node trust, and that the server node A now trusts, as now being a server-trusted node, and the untrust-list is reduced with said node, e.g. server node A reclassifies node G as being a server trusted node and the untrust-list is reduced to J, K, and M.

The distribution of trust relations is now completed and the untrust-list is empty. Server node A has collected signed public keys from all nodes B-M within the ad hoc network 201 and sends a message to all nodes B-M comprising server node A's collected signed public keys from all the nodes B-M within the ad hoc network.

The nodes A-M within the ad hoc communication network 201 now have mutual trust relations and a secure ad hoc network is established.

Figure 4 shows yet another scenario of the present invention. In this scenario an ad hoc network 401 comprises two trust groups 402 and 403 which shall be merged to one trust group constituting a secure ad hoc network. The first trust group 402 comprises a set of nodes, N, O, P, Q and R, all having mutual trust relations. The second trust group 403 comprises a set of nodes, S, T, U, V and W, all having mutual trust relations and which all are candidate nodes for joining the first trust group 402. The trust relations are created with trusted public keys. A node P is decided to act as a server node P within the first trust group 402 and a candidate node S is decided to act as a server node S within the second trust

group. According to the invention, the nodes N-W are authorised to delegate trust relations to other nodes within the network that it trusts.

Server node S sends a message, comprising a list of all candidate nodes S, T, U, V and W within the second trust group 403 and their corresponding public keys, to server node P. First server node P checks if it trusts any of the obtained keys, i.e. if it has trust relations to any of the candidate nodes S, T, U, V and W. First server node P, then classifies the candidate nodes as being first server-trusted nodes or as being first server-untrusted node, in this case P-trusted or P-untrusted.

If the classification results in at least one first server-trusted node, a scenario comes up as illustrated in **figure 5**. In this scenario first server node P has a trust relation to the node W and first server node P sends a message to second server node S. The message comprises

- a list of all nodes N, O, P, Q and R within the first trust group 402 and their corresponding public keys, and
- a list of first server-trusted nodes, which in this case is the P-trusted node W, and its corresponding public key.

Second server node S obtains the message and signs it and forwards it to node W.

Node W receives the signed message and checks the signature of the message. If node W trusts the signature, node W

- signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402,
- sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first trust group 402 to all candidate nodes S, T, U and V within the second network,
- sends a signed message comprising all trusted public keys of the candidate nodes S, T, U, V and W to first server node P.

First server node P receives the message and checks the signature of the message. If it is valid, first server node P signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends them in a signed message to all nodes N, O, Q and R.

The nodes N-W within the ad hoc network 102 now have mutual trust relations and a secure ad hoc communication network is established.

In another scenario, shown in **figure 6**, the classification is resulting in no first server-trusted node i.e. a P-trusted node. This means that first server node P has no trust relation with any of the candidate nodes S, T, U, V and W. Server node P then asks the other nodes N, O, Q and R within the first trust group 402, one by one, until sever node P obtains a positive answer of the question, if they have a trust relation with any of the candidate nodes S, T, U, V and W, within the second trust group 403.

In this case, node N has no such trust relation, the query is forwarded to node O, which has not got such trust relation either. The query is forwarded to node Q, which has a trust relation with node V in the second trust group, and now the procedure of distributing trust can start.

Node Q sends a signed message to second server node S. The message comprises:

- a list of all nodes N, O, P, Q and R within the first trust group 402 and their corresponding public keys,
- a list of the nodes that node Q trusts, which in this case is the node V, and its corresponding public key.

Second server node S obtains the message and forwards it to node V.

Node V receives the signed message and checks the signature of the message. If node V trusts the signature, it signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402. Node V then sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first trust group 402 to all candidate nodes S, T, U and W within the second network. Node V sends a signed message comprising all trusted public keys of the candidate nodes S, T, U, V and W to node Q.

Node Q receives the message and checks the signature of the message. If it is valid, node Q signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends the keys in a signed message to the other nodes N, O, P and R within the first trust group 402.

The nodes N-W within the ad hoc network 102 now have mutual trust relations and a secure ad hoc communication network is established.

In yet another scenario, none of the nodes N, O, P, Q and R, within the first trust group 402, have a trust relation with any of the candidate nodes S, T, U, V and W, within the second trust group 403. In this case a message is returned to first server node P asking node P to manually create a trust relation with the second server node S. This scenario is illustrated in **figure** 7. First server node P and second server node S now constitute a trust group 701.

First server node P sends a message to second server node S. The message comprises a list of all nodes N, O, P, Q and R, within the first trust group 402, and their corresponding public keys.

Second server node S

– signs the received public keys of the nodes N, O, P, Q and R within the first trust group 402,

- sends a signed message comprising the signed public keys of the nodes N, O, P, Q and R within the first trust group 402 to all candidate nodes S, T, U and V within the second network,
- sends a signed message comprising all trusted public keys of the candidate nodes S, T, U, V and W to first server node P.

First server node P receives the message and checks the signature of the message. If it is valid, first server node P signs the public keys of the candidate nodes S, T, U, V and W within the second trust group 403 and sends them in a signed message to all nodes N, O, Q and R.

The nodes N-W within the ad hoc communication network 102 are now having mutual trust relations and a secure ad hoc network is established.